"A Tribe of Excellence"

Digital Citizenship Event

phishing: when people send you phony emails, pop-up messages, social media messages, texts, calls, or links to fake websites in order to hook you into giving out your personal and financial information

How to Catch a Phish *(15 minutes)*

ASK:

How do you think identity thieves might try to get your information?

Encourage students to share some responses, even if they have not previously encountered identity theft.

DEFINE the Key Vocabulary term **phishing**.

EXPLAIN to students that the best way to avoid phishing scams is to be skeptical about any online request for personal information. It's also good to be skeptical of online messages or posts from friends that seem out of character for them, which is a warning sign that their accounts have been hacked. There are clues that can help students spot phishing, and they will learn some of these in the next part of the lesson by studying one type of phishing scam: a phony email message.

DIVIDE students into pairs.

DISTRIBUTE the **Spotting Scams Student Handout**, one per student.

READ aloud the instructions found on the **Spotting Scams Student Handout – Teacher Version**, and share with students the extended explanation of each feature of a phishing email.

INSTRUCT student pairs to complete the handout together. When students are done, have two pairs get together to exchange their handouts and compare their answers.

INVITE volunteers to share their answers with the class. Use the **Spotting Scams Student Handout – Teacher Version** for guidance.

REMIND students that phishing emails can be very convincing, and some may not contain many of the clues they just learned about. So it's smart to distrust any email that asks them to provide private information.